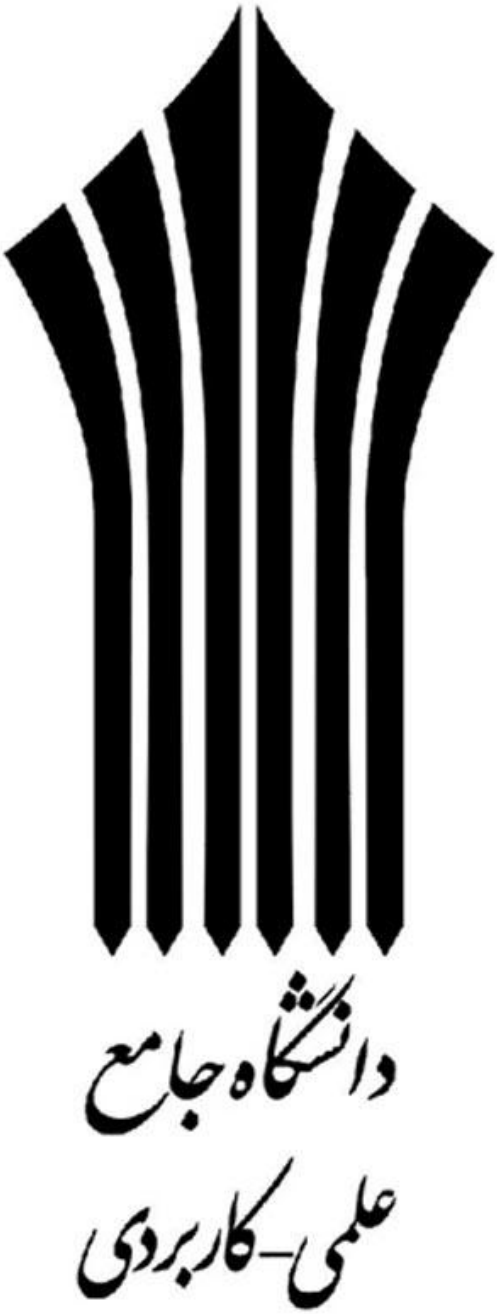


مرکز آموزش علمی کاربردی دزفول یک

مفاهیم TCP/IP

مدرس : رضا فرشیدی

interq.blogfa.com

شبکه کامپیوتری : مجموعه ای از کامپیوترهای مستقل و مرتبط به هم

پروتکل : مجوعه ای از قوانین و مقررات ها برای ارتباط بین کامپیوترها

پهنای باند : میزان داده ای که در واحد زمان می توان از یک کانال ارتباطی عبور داد و وابسته به کانال ارتباط فیزیکی است

خدمات(Services) :

1) اتصال گرا (connection oriented)

2) بدون اتصال(connectionless)

مزایای شبکه :

بالا بردن کارایی، کاهش هزینه،از بین بردن محدودیت جغرافیایی، اشتراک گذاری منابع

انواع شبکه :

1) از نظر جغرافیایی :
- LAN
- MAN
- WAN

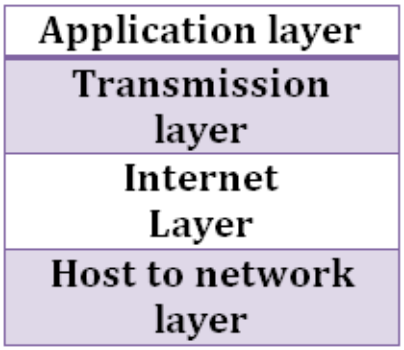
2) از نظر تکنولوژی انتقال :
- Broad cast
- Point to point

مدل معرفی شده برای شبکه های کامپیوتری توسط سازمان استاندارد جهانی :

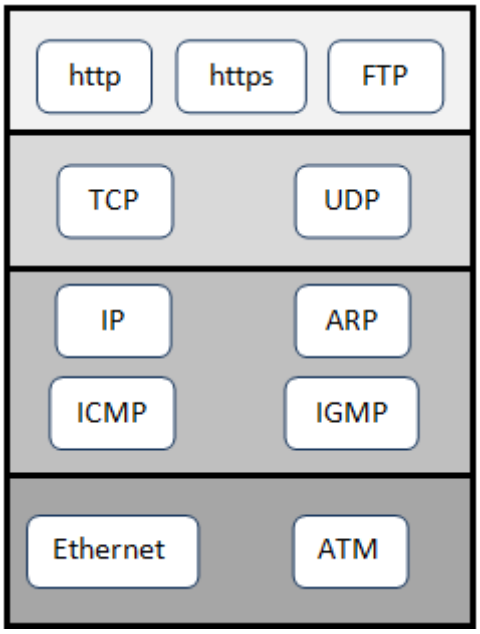
مدل OSI : لایه ها : کاربرد ، نمایش ، جلسه ، انتقال ، شبکه ، پیوند ، فیزیکی

Application layer
Presentation layer
Session layer
Transmission layer
Network layer
Data link layer
Physical layer

مدل TCP/IP : لایه ها : کاربرد، انتقال، اینترنت، میزبان با شبکه



پروتکل های موجود در لایه های TCP/IP



لایه انتقال : لایه انتقال قابلیت ایجاد نظم و ترتیب و تضمین ارتباط بین کامپیوترها و ارسال داده به سمت لایه های بالای لایه خود را دارد در این لایه دو پروتکل بسیار مهم معرفی شده است TCPو UDP

پروتکل TCP : (**T**ransmission **C**ontrol **P**rotocol)

این پروتکل مسئول تضمین صحت ارسال اطلاعات است. به این منظور با ارسال هر بسته (packet) گیرنده باید یک رسید(ack) برای فرستنده ارسال کند تا مطمئن شود آن بسته به مقصد رسیده است. در کاربردهایی که برای ما درست رسیدن مهم باشد از این پروتکل استفاده می کنیم

پروتکل UDP : (**U**ser **D**atagram **P**rotocol)

این پروتکل داده را به صورت سریع ولی بدون تضمین صحت ارسال اطلاعات به سمت گیرنده ارسال می کنددر کاربردهایی که سرعت از دقت مهم تر است از این پروتکل استفاده می کنیم. (مثل ارسال ویدئوهای زنده در اینترنت)

لایه اینترنت :

مسئولیت آدرس دهی، مسیریابی و بسته بندی داده ها را بر عهده دارد

این لایه شامل چهار پروتکل مهم است :

1) پروتکل IP : (**I**nternet **P**rotocol)

این پروتکل مسئول آدرس دهی داده ها به منظور ارسال به مقصد مورد نظر است.

2) پروتکل ARP :

این پروتکل مسئول مشخص نمودن آدرس MAC ، معروف به آدرس مربوط به آداپتور شبکه بر روی کامپیوتر مقصد است.

3) پروتکل ICMP : (**I**nternet **C**ontrol **M**essage **P**rotocol)

این پروتکل مسئول ارایه توابع عیب یابی و گزارش خطا در صورت عدم توزیع صحیح اطلاعات است

4) پروتکل IGMP : (Internet Group Management Protocol)

این پروتکل وظیفه مدیریت ارسال چند بخشی(Multi cast) را بر عهده دارد.

لایه میزبان شبکه:

پروتکلATM : (Asynchronous Transfer Mode)

حالت انتقال به صورت غیر همزمان

آدرس های IP :

آدرس های IPدر حالت کلی از دو بخش Network ID و Host ID تشکیل می شوند.

نکته) آدرس های تماما صفر و تماما یک جهت کاربردهای خاص هستند.

کلاس های آدرس IP :

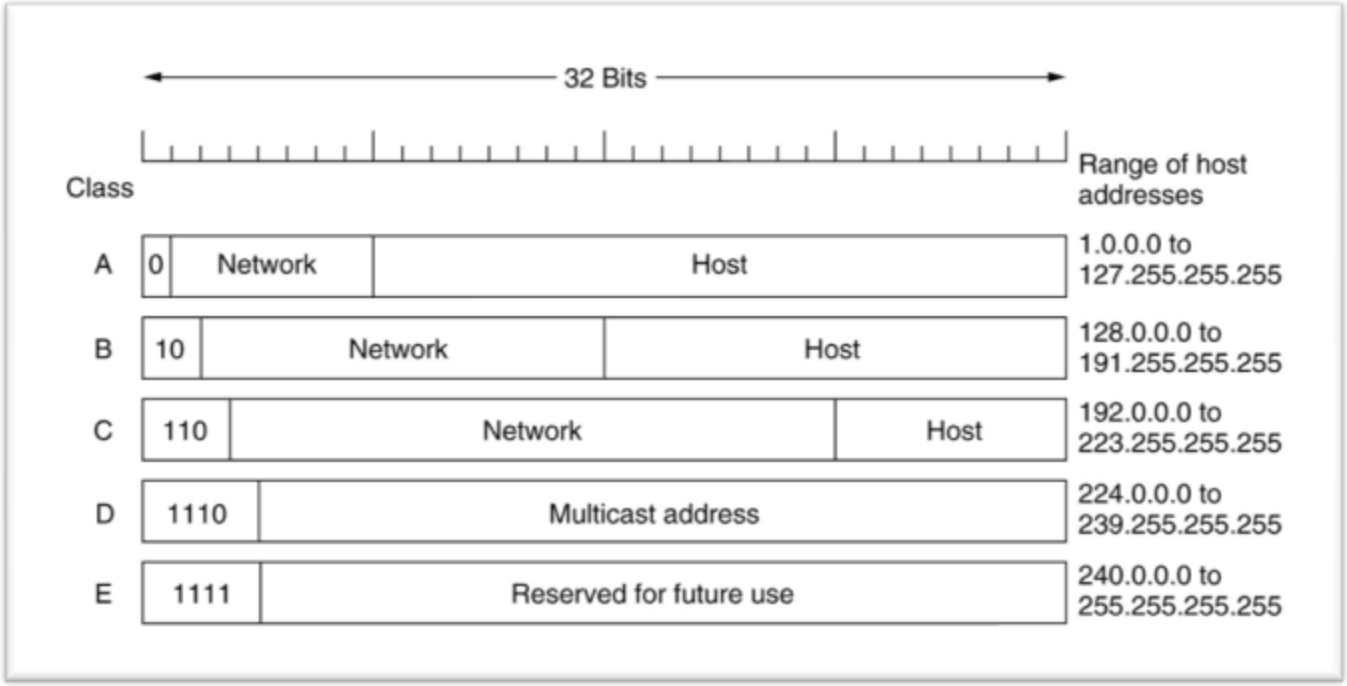
کلاس های IP به پنج کلاس تقسیم میشوند: A , B , C , D , E و هرکلاس دارای مشخصاتی است که در جداول زیر نشان داده شده است :

به عنوان نمونه مشخصات **کلاس A** بدین شرح است :

7 بیت آدرس شبکه (Network) و 24 بیت برای آدرس میزبان(Host) – (بیت اول آدرس شبکه رزرو است)

اولین آدرس میزبان 1.0.0.0 و آخرین آدرس میزبان 127.255.255.255

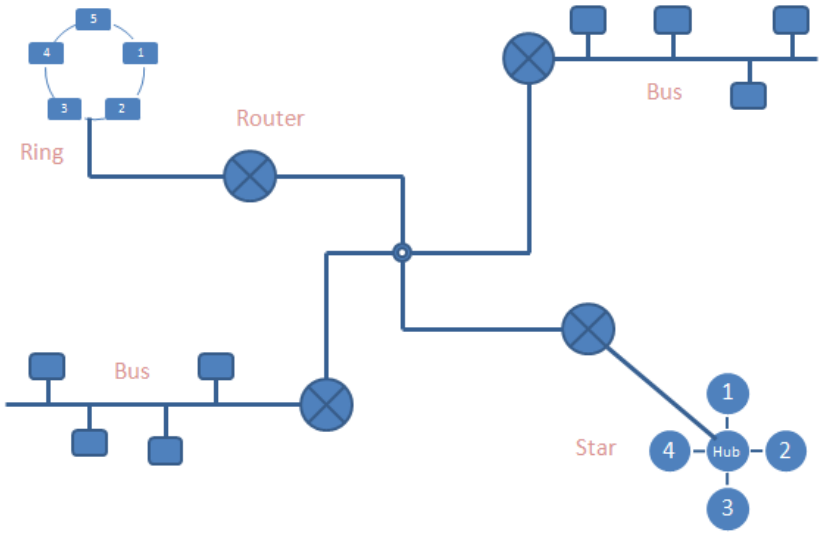
تعداد شبکه 125 و تعداد میزبان 16.777.214



Class	*IP address range (1st Octet)*	*Network Mask*	*Prefix*	*Number of Networks*	*Number of Hosts*
A	1. - 127.	255.0.0.0	/8	125	16,777,214
B	128. - 191.	255.255.0.0	/16	16,382	65,534
C	192. - 223.	255.255.255.0	/24	2,097,150	254
D	224. - 239.	Multicast addresses			
E	240. - 254.	Restricted/Experimental			

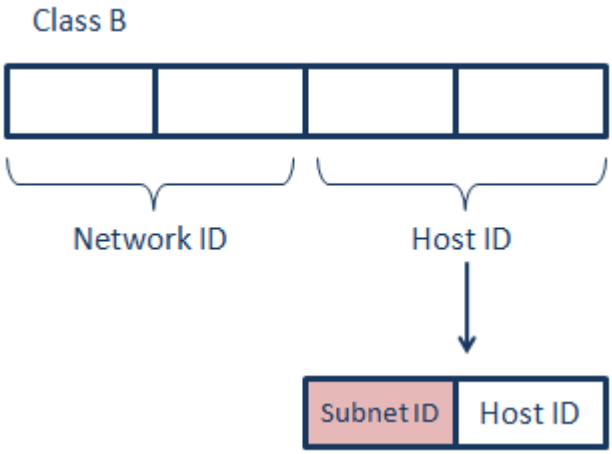
کلاس های D و E جهت کاربردهای خاص هستند.

در بحث مربوط به کلاس بندی آدرس های IP در برخی از کلاس ها مانند A و B تعداد کامپیوترهای میزبان نسبتا زیاد بوده و مدیریت یکپارچه آنها تحت یک شبکه LAN بسیار مشکل است. به همین منظور باید با استفاده از روشی بتوانیم این شبکه های بزرگ را به شبکه های کوچکتر و LAN های جداگانه تقسیم کنیم که به این منظور از مفهوم زیرشبکه بندی یا Subneting استفاده می کنیم. مانند شکل زیر :



برای درک شبکه بندی باید مفهوم الگوی زیرشبکه یا Subnet Mask را هم بدانیم. الگوی زیرشبکه همانند آدرس های IP به صورت ترکیبی از بیت های صفر و یک، به گونه ای انتخاب می شوند که قسمت شبکه و هاست را برای ما مشخص کنند

در الگوهای زیرشبکه به صورت استاندارد، مقادیر بایت ها یا تماما یک است یا صفر



مثال :

142	15	27	14
255	255	255	0
Network ID		Subnet ID	Host ID

اگر بایت سوم 255 بود، از زیرشبکه استفاده شده است.

مثال برای حالت استاندارد) فرض کنید که در یک سازمان با کلاسB بخواهیم حداکثر 254 زیر شبکه تعریف کنیم. الگوی زیرشبکه به چه شکلی باید باشد؟

$254+2=256 \rightarrow 2^8$ (به هشت بیت برای آن نیاز داریم)

1111 1111	1111 1111	1111 1111	0000 0000
255	255	255	0
Network ID		**Subnet ID**	Host ID

مثال برای حالت غیراستاندارد)فرض کنید در یک سازمان با کلاس از نوعB بخواهیم حداکثر 28 زیر شبکه با تعداد هزار میزبان برای هر کدام تعریف کنیم. الگوی زیرشبکه را رسم کنید؟

نکته) نباید الگوی زیر شبکه را دقیقا طوری طراحی کنیم که دقیقاهزار تا شود، بلکه باید الگو را برای مقادیر بیشتری طراحی کنیم

$28+2=30$(زیر شبکه) $\rightarrow$ 2^5(حداقل پنج بیت نیاز است)

$2^{11}-2=2046$ (تعداد کامپیوترهای میزبان شبکه)

Network ID		**Subnet ID**	Host ID	
1111 1111	1111 1111	11111	000	0000 0000
255	255	248		0

برای دانستن اینکه دو کامپیوتر در یک LAN قرار دارند باید آدرس زیر شبکه (دودویی) را در آدرس مبدا و مقصد AND کنیم. اگر جواب ها یکسان باشد دو کامپیوتر در یکLAN قرار دارند.

مثال)در ادامه مثال قبلی اگر آدرس مبدا 135.17.231.12 و آدرس مقصد 235.17.224.15 باشد تعین کنید که دو آدرس متعلق به یک LAN هستند؟

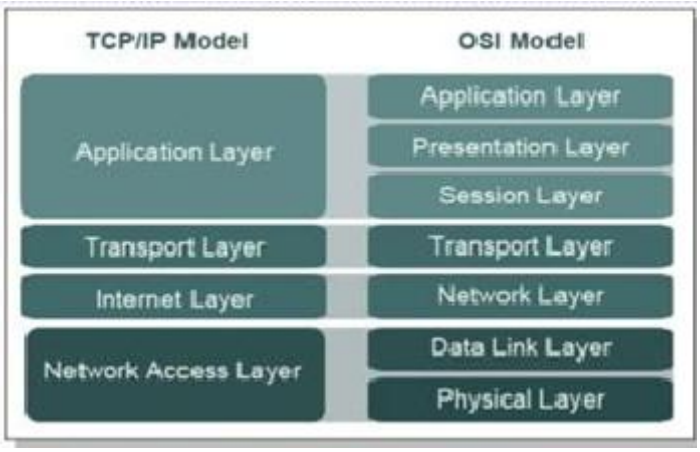
آدرس مقصد			
1111 1111	1111 1111	1111 1000	0000 0000
1000 0111	0001 0001	1110 0000	0000 1111
1000 0111	**0001 0001**	**1110 0000**	**0000 0000**

جدول AND
1.1=1
1.0=0
0.1=0
0.0=0

آدرس مبدا			
1111 1111	1111 1111	1111 1000	0000 0000
1000 0111	0001 0001	1110 0111	0001 1000
1000 0111	**0001 0001**	**1110 0000**	**0000 0000**

چون نتیجه هر دو یکسان شده است پس روی یکLAN قرار دارند.

لایه های مختلف در مدل TCP/IP



لایه واسط شبکه در مدل TCP/IP معادل دو لایه فیزیکی و پیوند داده در مدلOSI است. وظایف این لایه :

1. ایجاد یک کانال بدون خطا از دید لایه بالاتر(کنترل خطا، کنترل جریان و ...)
2. ارسال دیتا از هر یک از کانال های ارتباطی

ارتباطات در این لایه به صورت انجام می گیرد(قرار دادن داده ها روی کانال ارتباطی) :

1. نقطه به نقطه با لینک اختصاصی
2. ارسال داده بر روی کانال مشترک

استانداردهای(پروتکل ها) انتقال داده رو خطوط نقطه به نقطه(مثل سیم تلفن) :

SLIP	**S**erial **L**ink **I**nternet **P**rotocol
PPP	**P**oint to **P**oint **P**rotocol

پروتکل SLIP :

یک پروتکل بسیار ساده جهت ارسال بین مبدا و مقصد به صورت نقطه به نقطه است در این روش هر کامپیوتری که بخواهد داده ارسال کند، یک کاراکتر خاص که نشان دهنده شروع ارسال داده است ر روی خط می فرستد و پس از آن اقدام به ارسال داده می کند. پس از پایان ارسال داده، همان کاراکتر خاص مجددا ارسال می شود که نشان دهنده اتمام ارسال داده است.

قاب یک فریم در این روش :

اشکالات این روش :

1. اگر کاراکتر 0c (صفر سی) در داده های ما وجود داشته باشد، برای اینکه سیستم گیرنده به اشتباه آنرا به عنوان انتهای داده‌ها تلقی نکند از ابتدا آنرا به زوج کاراکترهای DB (سی) و DC (صفر) جایگزین می کند

مثال :

18	32	0C	25	DB	DC	14
↓	↓	↓	↓	↓	↓	↓
18	32	DB DC	25	DB	DC	14
↓	↓	↓	↓	↓	↓	↓
18	32	DB DC	25	DB DD	DC	14

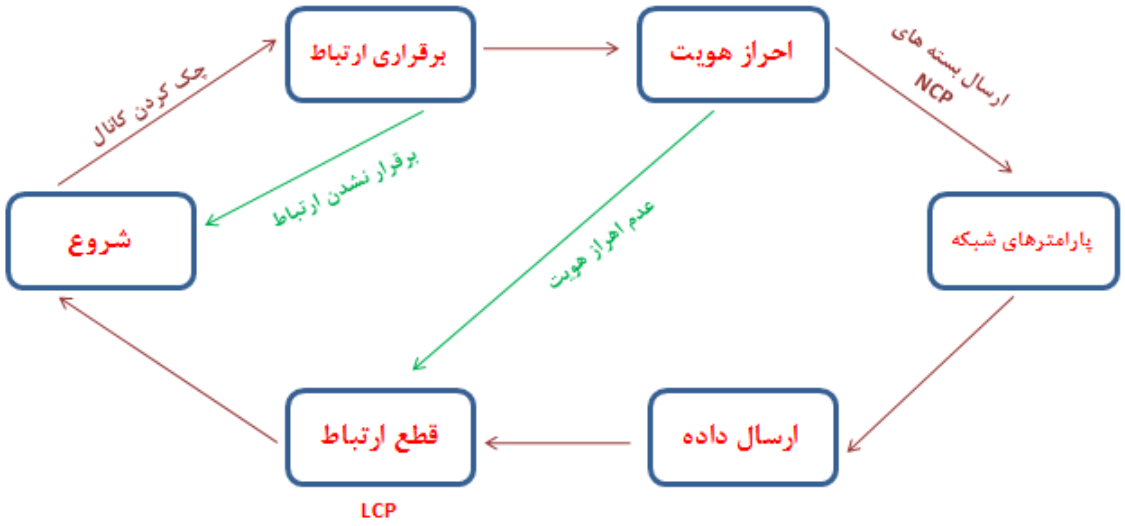
2. هیچ مکانیزمی برای کشف خطا وجود ندارد.
3. در این پروتکل بحث وجود آدرس IP بین مبدا و مقصد مطرح نشده است و بنابراین نمی توان آنرا در هر شبکه ای استفاده کرد
4. ماشین های فرستنده و گیرنده روش خاصی برای احراز هویت ندارند و همین مسئله امنیت را کم می کند بنابراین پروتکل دیگری به نام PPP تعریف شده است که تحدودی اشکالات فوق را بر طرف می کند.

پروتکل PPP :

Flag	Address	Control	Protocol	Data	Checksum	Flag
یک بایت	**یک بایت**	**یک بایت**	**یک تا دو بایت**	متغیر	**دو تا چهار بایت**	**یک بایت**

در این پروتکل برای ایجاد یک ارتباط، ابتدا بسته های خاصی بنامLCP ارسال می شوند که به وسیله آنها لینک بین مبدا و مقصد اختصاص داده خواهد شد و همچنین برخی پارامترهای پروتکل PPP انتخاب و تنظیم می شود. پس از آن با ارسال بسته هایNCP برخی پارامترهای شبکه برای ارتباط از جمله طول فیلد دیتا مشخص می شود و همچنین یک آدرسIP موقت برای کامپیوترها تنظیم می شود و سپس اقدام به ارسال داده می کند.

پس از پایان ارسال داده ها، باز یک بستهNCP فرستاده می شود تا آدرسهای IP گرفته شده، آزاد شود و با یک بستهLCP ارتباط لینک به صورت فیزیکی قطع می شود. مراحل انجام این کار به صورت زیر می تواند نمایش داده شود :



کانال های اشتراکی :

تاکنون دو پروتکل PPP و SLIP را برای کانال های نقطه به نقطه مطرح کردیم. اما در کانال های اشتراکی بدلیل امکان برخورد بین بسته های اطلاعاتی، الگوریتم های متفاوتی برای مدیریت آن ها مطرح شده است.

مدیریت کانال :

1. ALOHA محض :

در این روش هر ماشینی در شبکه می تواند در هر زمان دلخواه اقدام به ارسال فریم های داده کند. در صورتی که قاب های داده از دو یا چند ماشین با هم برخورد کنند، این موضوع به اطلاع فرستنده رسیده و آنها نیز پس از یک مدت زمان تصادفی اقدام به ارسال مجدد فریم های هاه می کنند.(کارایی حدود 18%)

2. ALOHA برهه ای :

(Slotted Aloha) در این روش برخلاف روش محض، هر سیستمی نمی تواند در هر زمان دلخواه اقدام به ارسال کند. بلکه برهه یا اسلات های زمانی در نظر گرفته شده و هر سیستمی در اسلات مربوط به خود می تواند قاب های داده را ارسال کند. در این حالت نیز امکان برخورد وجود دارد اما میزان آن کمتر است، به صورتی که کارایی نسبت به روش محض حدود دو برابرمی شود.

3. پروتکل CSMA/CD

Carier **S**ense **M**ultiple **A**ccess with **C**ollision **D**etection

گوش دادن به رسانه مشترک و دسترسی چند گانه به همراه تشخیص برخورد

در این پروتکل کامپیوترهایی که می خواهند داده ارسال کنند، ابتدا به کانال اشتراکی گوش می دهند(سنس کردن) و سپس اقدام به ارسال داده می کنند. چنانچه در این حالت برخوردی پیش آید، دو یا چند سیستمی که برخورد داشتند باید تا یک مدت تصادفی صبر کرده و مجددا اقدامب ارسال داده کنند.

هر چه پهنای باند بیشتر شود کارایی کمتر می شود	پهنای باند	B
هر چه طول کانال اشتراکی بیشتر شود کارایی کمتر می شود	طول کانال اشتراکی	L
هر چه طول فریم کمتر شود کارایی کمتر می شود	طول فریم	F
عدد ثابت	سرعت انتشار	C
عدد ثابت=2.7	عدد نپر	e

نکته) سوال امتحانی به صورت محاسبه کارایی داده نمیشود وتاثیر اجزا بر کارایی پرسیده خواهد شد.

کنترل خطا :

کنترل خطا	کدهای توازن (parity)	زوج	فقط جهت تشخیص خطا
		فرد	
	کد همینگ	جهت تشخیص و تصحیح خطا	

کدهای توازن :

یکی از روش های تشخیص خطا، استفاده از بیت توازن است. این بیت به نحوی به رشته داده اضافه می شود که تعداد بیت های موجود در آن در نهایت زوج(برای توازن زوج) و یا فرد (برای توازن فرد) شود. این بیت در مبدا و مقصد مقایسه شده و در صورت داشتن تفاوت می فهمیم که دچار خطا شده است. یکی از اشکالات این روش آنست که ما در توازن زوج، امکان تشخیص خطاهایی با تعداد زوج را نداریم. این قضیه برای توازن فرد هم وجود دارد اما برعکس.

01110	داده
0	بیت توازن

فاصله همینگ :

به تعداد بیت هایی که بین دو رشته بیتی، متفاوت باشند فاصله همینگ می گویندآنرا با d نمایش می دهند.

رشته اول	1111 0000	d=4
رشته دوم	1111 1111	

نکته) در کدهای با فاصله همینگ d امکان تشخیص خطا (d-1) و تصحیح خطا $[\frac{d-1}{2}]$ وجود دارد.

اگر d=1	
تشخیص خطا	d-1=4-1=3
تصحیح خطا	$[\frac{d-1}{2}]= [\frac{4-1}{2}]=[1.5] = 1$

برای تصحیح خطا معمولا اگر یک رشته بیتی با طول m وجود داشته باشد، r بیت افزونه اضافی که آنرا بیت های کنترلی می گویند به دیتای اصلی اضافه می شود. مکان در نظر گرفته شده برای بیت های کنترلی، مکان هایی است که توان هایی از عدد2 باشد. ..., 8 , 4 , 2 , 1

لازم به ذکر است که بیت های داده در سایر مکان ها قرار می گیرد.

نکته) مقدار بیت های کنترلی ما از XOR نمودن تعدادی از بیت های داده به دست می آید. در جدول XOR اگر تعداد یک ها فرد باشد جواب، یک است و اگر تعداد یک ها زوج باشد، حاصل صفر می شود

جدول XOR
0.0=0
0.1=1
1.0=1
1.1=0

سوال) مقدار بیت های کنترلی را بدست آورید؟ (اعداد رشته داده، بعد از کدهای همینگ قرار می گیرند.)

رشته داده	1101 0011

بیت ها	C1	C2	1	C4	1	0	1	C8	0	0	1	1
	1	2	3	4	5	6	7	8	9	10	11	12

	C8	C4	C2	C1
1	0	0	0	1
2	0	0	1	0
3	0	0	1	1
4	0	1	0	0
5	0	1	0	1
6	0	1	1	0
7	0	1	1	1
8	1	0	0	0
9	1	0	0	1
10	1	0	1	0
11	1	0	1	1
12	1	1	0	0

C1	=	3©5©7©9©11	=	1©1©1©0©1	=	0
C2	=	3©6©7©10©11	=	1©0©1©0©1	=	1
C4	=	5©6©7©12	=	1©0©1©0	=	1
C8	=	9©10©11©12	=	0©0©1©1	=	0

رشته بیت های نمایه ارسالی	0	1	1	1	1	0	1	0	0	0	1	1
	C1	C2		C4				C8				

سوال) این رشته بیت ارسال شده است. تشخیص دهید که این کد دچار خطا شده یا نه؟ و در کدام بیت؟

رشته داده	011110000011

C1	=	1©3©5©7©9©1	=	0©1©1©0©0©1	=	1
C2	=	2©3©6©7©10©11	=	1©1©0©0©0©1	=	1
C4	=	4©5©6©7©12	=	1©1©0©0©1	=	1
C8	=	8©9©10©11©12	=	0©0©0©1©1	=	0

برای اینک تشخیص دهیم در کدام بیت دچار خطا شده ایم، کدهای همینگ را از آخر به اول می نویسیم و یک کد دودویی بدست می آید (0111) . این کد را به دهدهی تبدیل می کنیم تا بفهمیم در کدام بیت خطا داریم

0111=7 بیت هفتم خراب است

نکته) اگر تمام جواب های بدست آمده در همینگ برابر صفر شود، در این رشته بیت، خطا نداریم.

کنترل جریان :

در واقع جلوگیری از افتادن یک گیرنده کند در دام یک فرستنده سریع است و در این حالت مقداری از داده ها از بین خواهد رفت برای کنترل جریان دو روش کلی وجود دارد :

1. کنترل بر اساس بازخورد :

در این حالت گیرنده کند، عدم توانایی خود برای تطابق با فرستنده‌را به وی اعلام می کند بنابراین فرستنده بر این اساس خود را با گیرنده هماهنگ می کند.(فرستنده خود را کند می کند)

2. استفاده از کنترل جریان بر اساس میزان :

در این روش به دو طریق فرستنده و گیرنده هماهنگ می شوند یا هر دو از ابتدا در مورد مقدار دیتای ارسالی بین خود در یک زمان مشخص توافق می کنند و یا اینکه فرستنده مقدار مشخصی داده برای گیرنده می فرستد و متوقف می شود تا گیرنده مجددا برای دریافت اعلام آمادگی کند.

نکته) مطالب گفته شده اخیر مربوط به لایه واسط شبکه بود در ادامه در مورد لایه اینترنت بحث خواهد شد

لایه اینترنت :

وظایف : آدرس دهی، سوئیچینگ، مسیریابی، عملیات کپسول سازی و قطعه بندی

قالب یک بسته IP v4 در لایه اینترنت :

Version	IHL	Type of service	Total lenght		
Identification			DF	MF	fragment offset
Time to live	Prtocol		Header check sum		
Source IP adress					
Destination IP adress					
Option					
Data (pay lead)					

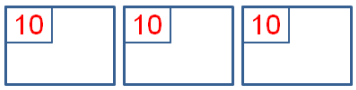
Version : (چهار بیت است) این فیلد نسخه پروتکل IP را مشخص می کند.(نسخه 4 یا نسخه 6)

IHL (internet head line) : طول سرآیند یک بسته IP را مشخص می کند.(چهار بیتی است).

Type of service : (هشت بیتی است) در صورتی که یک بسته در هنگام عبور از مسیریاب ها نیاز به یک سرویس خاص داشته باشد، نوع آن سرویس در این بخش مشخص می شود.(مثل ارسال در کوتاهترین مسیر یا سریعترین روش ارسال)

Total lenght : (شانزده بیتی است) این فیلد مشخص کننده حداکثر طول یک بسته IP است

Identification : (شناسه)(16 بیتی است)زمانی که یک پیام به دلیل بزرگ بودن، قطعه بندی شود، برای اینکه بدانیم کدام قطعه ها متعلق به چه پیامی هستند بایدبه همه آنها یک شماره یکسان و خاص بدهیم

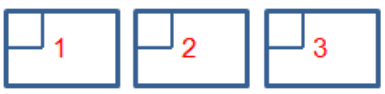


نکته) پس از این فیلد، یک فیلد یک بیتی خالی وجود دارد

DF : (don’t fragment)(یک بیتی است) اگر یک پیام به هر دلیلی نخواهد قطعه بندی شود

MF: (more fragment) مشخص می کند که آیا بسته فعلی، آخرین قطعه از یک قطعه بندی است یا پس از آن قطعات بیشتری وجود دارند. در صورتی که این بیت یک باشد یعنی آخرین قطعه است و اگر صفر باشد پس از آن قطعات دیگری نیز وجود دارند

fragment offset : (13 بیتی است) این فیلد، شماره یک قطعه را در یک عملیات قطعه بندی مشخص می کند تا بر اساس آن قطعات به ترتیب کنار هم قرار گرفته و بازسازی شوند.



Time to live : (هشت بیتی است) این بیت زمان حیات یک بسته را مشخص می کند چنانچه یک بسته در طول عمر خود نتواند به مقصد برسد، حذف شده و به این ترتیب اجازه سرگردان شدن آن در شبکه داده نخواهد شد

$2^8 = 256$ زمان مختلف

Protocol : (هشت بیتی است) این فیلد، پروتکل لایه بالاتر که داده را بهIP تحویل داده، مشخص می کند که قاعدتا یکی از دو پروتکلTCP و UDP است.

checksum : (شانزده بیتی است) برای کنترل خطاست.

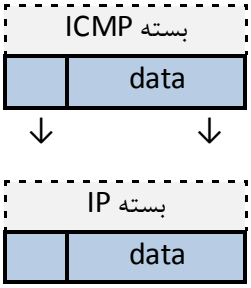
پروتکل ICMP :

Internet **C**ontrol **M**essage **P**rotocol

این پروتکل وظیفه گزارش خطا از طریق ارسال پیام هایی به فرستنده را فراهم می کند لازم به ذکر است که این پروتکل خود، کنترل خطا را انجام نمی دهد بلکه فقط گزارش آن را ارسال می کند.

به عنوان مثال در صورتی که پروتکلIP قادر به توزیع یک بسته به مقصد نباشد،ICMP یک پیغام مبتنی برغیر قابل دسترسی بودن را برای کامپیوتر مبدا ارسال می کند. این پروتکل با این وجود بازهم نمی تواند پروتکل غیرقابل اطمینانIP را مطمئن نماید. به این دلیل که پیام های ICMP هیچ گونه مکانیزمی برای اعلام وصول بسته ندارد

بسته های ICMP خود در قالب یک بستهIP ارسال می شوند.



قالب یک بستهICMP :

type	cod	checksum
parameters		
data		

type : نوع پیغام را مشخص می کند.

cod : اگر یک پیغام خود دارای پیا هایی باشد(زیر پیام) در این بخش مشخص می شود.

checksum : کنترل خطا

وظایف مهم لایه اینترنت :

1. سوئیچینگ (Switching)
2. مسیریابی (Routing)

مدل های سوئیچینگ :

1. سوئیچینگ مداری (Circuit Switching)
2. سوئیچینگ پیام (Message Switching)
3. سوئیچینگ بسته (Packet Switching)

سوئیچینگ مداری :

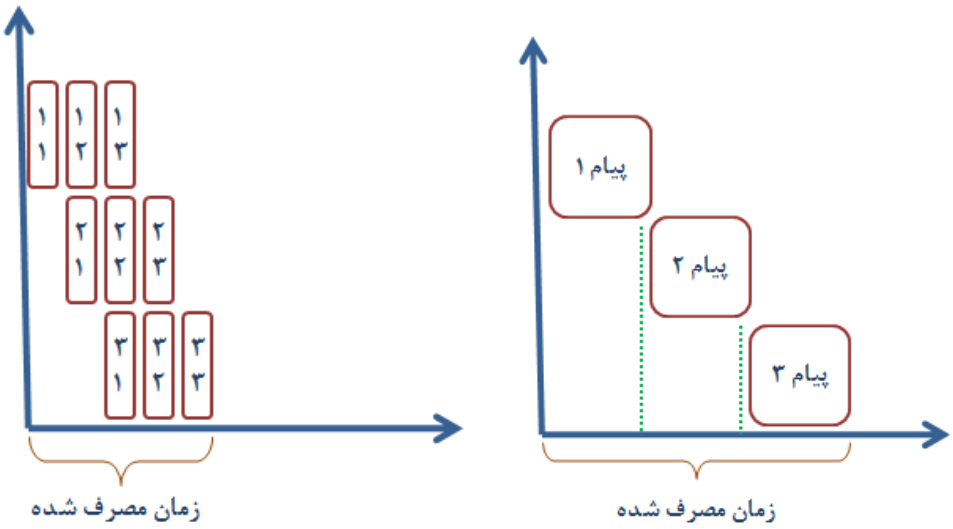
در این روش بین مبدا و مقصد، ابتدا یک مسیر ایجاد شده (رزرو شده) و پس از آن داده ها ارسال می گردند. این روش به دلیل ایجاد مسیر اختصاصی، قابل اطمینان بوده و سرعت مناسبی دارد اما در عین حال هزینه نگهداری مسیر نیز بالاست

سوئیچینگ پیام:

بر خلاف روش قبلی برای ارسال داده ها، نیاز به یک مسیر مشخص نیست و داده‌ها در قالب پیام هایی از هر مسیر دلخواه می توانند ارسال شوند. واضح است که در این حالت هزینه کمتر و در عین حال قابلیت اطمینان نیز کمتر است

سوئیچینگ بسته :

این روش همانند سوئیچینگ پیام عمل می کند با این تفاوت که پیام ها به بسته های کوچکتری بنام Packet شکسته شده و ارسال انجام می شود. این امر منجر به افزایش سرعت می شود.



مسیریابی : (Routing)

الگوریتم های مسیریابی :

1. الگوریتم های وفقی (Adaptive)
2. الگوریتم های غیر وفقی (Non Adaptive)

الگوریتم های غیر وفقی:

الگوریتم هایی هستند که جهت انجام مسیریابی و تصمیم‌گیری در مورد آن بر اساس وضعیت فعلی شبکه چه از نظر تخمین هم بندی(توپولوژی) یا ترافیک شبکه استوار نیست. مسیریابی هایی که توسط چنین الگوریتم هایی صورت می گیرد، مسیریابی ایستا(غیر فعال) نام دارد.

الگوریتم های وفقی:

این الگوریتم ها برای بهینه کردن مسیریابی،مواردی همچون وضعیت فعلی شبکه از نظر ترافیک و هم بندی را در نظر گرفته و مسیریابی آنها یک مسیریابی پویا (فعال) است.

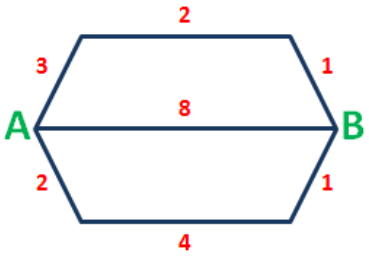
مسیریابی ایستا :

1. مسیریابی کوتاهترین فاصله
2. مسیریابی سیل آسا

مسیریابی کوتاه ترین فاصله :

الف) بر اساس هزینه و فاصله جغرافیایی: در این حالت معمولا یک گراف از مسیرهای موجود شبکه ایجاد شده و به هر یال آن، یک هزینه اختصاص داده می شود.

ب) بر اساس تعداد گام تا مقصد : در این حالت کوتاه ترین مسیر جهت انتقال داده ها انتخاب می شود



براساس هزینه	مسیر بالا	3+2+1=6	√
	مسیر وسط	8	
	مسیر پایین	2+4+1=7	

براساس تعداد گام	مسیر بالا	سه گام	
	مسیر وسط	یک گام	√
	مسیر پایین	سه گام	

مسیریابی سیل آسا :

در این مسیریابی برای ارسال یک بسته داده به سمت مقصد، آن بسته به تمامی خط های خروجی ارسال می شود بنابراین تعداد بسیار زیادی بسته که در واقع نیازی به آنهانداریم در شبکه ایجاد می شود. هرگاه یک بسته به مقصد برسد سایر بسته های مشابه باید از بین برودبه این منظور می توانیم بیشترین فاصله ای که دو گره از شبکه با هم دارند (قطر شبکه) را به عنوان حداکثر تعداد گام برای یک بسته قرار دهیم با هر بار عبور یک بسته از گره های میانی، مقدار گام آن یک واحد افزوده شده و پس از اینکه به آن مقدا حداکثر رسید، از بین خواهد رفت مگر اینکه در آن لحظه در مقصد بوده باشد.

مسیریابی پویا(فعال) :

الف) فاصله بردار (Distance-Vector)

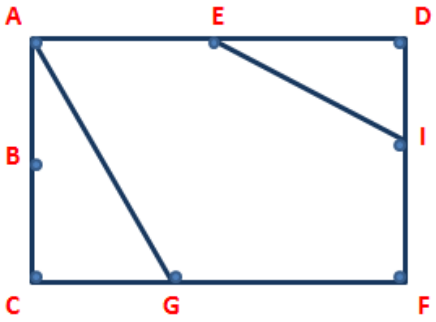
ب) حالت-پیوند (Link-State)

مسیریابی فاصله بردار :

در این روش نیز یک گراف از شبکه ایجاد می شود و سپس در هر گره (Node) آن، جداولی در نظر گرفته خواهد شد که این جداول شامل دو فیلد همسایه ها و همچنین فاصله تا هر همسایه است برای به دست آوردن این فاصله هر گره بسته خاصی به نامEcho به همسایگانش ارسال می کند و پس از بازگشت این بسته، فاصله پیموده شده تخمین زده می شود زمانی که یک فرستنده می خواهد برای یک گیرنده داده ارسال کند، با توجه به این جداول، بهترین مسیر که کمترین فاصله را دارد انتخاب خواهد نمود داده های موجود در جداول مرتبا بروز رسانی می شود.

B	
A	5
B	0
C	5
D	20
E	12
F	20
G	9
I	24

A	
A	0
B	5
C	10
D	15
E	7
F	25
G	15
I	19



یکی از اشکالات مسیریابی فاصله بردار این بودکه پهنای باند یا بار موجود بر روی مسیرهای مختلف را در نظر نمی گرفت بنابراین نمی توانست در شبکه های امروزی که ینک هایی با پهنای باند مختلف و بعضا بلا وجود داشت به خوبی عمل نمایدلذا یک مسیر یابی به نام حالت‌پیوند به وجود آمد که ترافیک و بار شبکه را در نظر می گرفت.

مسیریابی حالت-پیوند :

در این مسیریابی گره‌های زیر انجام می شود :

1. پیدا کردن تمامی همسایگان : به این منظور از بسته خاصی به نام سلام(Hello) استفاده می شود.
2. فاصله تا هر همسایه را به دست می آورد.(با استفاده از بسته Echo)
3. جدولی از اطلاعات تمامی همسایه ها فراهم شده و سپس آن را به صورت سیل آسا برای تمام گره های شبکه ارسال می کند و در نهایت از این جداول برای مسیریابی استفاده می شود. فرمت این جدول به صورت زیر است :

A	
Sequence	
Age	
A	0
B	15
C	16
D	8

Age : (سن) وقتی دو جدول با داده های مختلف برای یک گره استفاده می شود، جدولی در نظر گرفته خواهد شد که سنش کمتر باشد و عملا داده های آن بروزتر هستند.

Sequence : (شماره ترتیب)

لایه انتقال دارای دو پروتکل اصلی TCP و UDP است. پروتکل TCP اتصال گرا و پروتکل UDP بدون اتصال است. از پروتکل TCP برای ارسال هایی استفاده می شود که می بایست قابل اطمینان باشد مانند ارسال فایل هایی که در آنها بوز خطا جایز نیست. در عوض پروتکل UDP برای ارسال های کوچک یا سریع به کار می رود.

پروتکل های TCP و UDP برای انجام عملیات های مختلف از پورت های خاصی استفاده می کنند که برخی از آنها به شرح زیر است :

سرویس	شماره پورت	نام پروتکل	وظیفه
FTP-DATA	20	TCP	ارسال و دریافت فایل
FTP	21	TCP	درخواست و تبادل دستورات بین دو سیستم
SMTP	25	TCP	ارسال ایمیل
POP 3	110	TCP	دریافت ایمیل
HTTP	80	TCP	برای ارسال صفحات وب
DOMAIN	53	TCP/UDP	سرویس DNS
BOOT P	68	TCP/UDP	سرویس گیرنده Boot P و DHCP

کاربرد پروتکل DNS تبدیل آدرس دامین به IP است.

پروتکل DHCP :

Dynamic **H**ost **C**onfiguration **P**rotocol

در یک شبکه، کامپیوترها برای ارتباط با هم باید آدرسIP منحصر به فرد داشته باشند هر چند می شود این کار را با اختصاص آدرس ها ب صورت دستی انجام داد، اما هم امکان خطا وجود دارد و هم برای شبکه های بزرگ امکان پذیر نیست. به همین دلیل از پروتکلDHCP استفاده می شود که با ورود هر سیستم به شبکه به صورت اتوماتیک، یک آدرسIP اختصاص می دهد.

در صورت مشاهده هرگونه اشکال در مطالب این جزوه، آنرا ذکر و به ایمیل زیر ارسال نمایید.

rayanjack73@yahoo.com

آدرس وب :

interq.blogfa.com

با تشکر